Exhibit E

iCloud security overview

iCloud uses best-in-class security technologies, employs strict policies to protect your information, and leads the industry by adopting secure, privacy-preserving technologies like end-to-end encryption for your data.

Data security

iCloud secures your information by encrypting it when it’s in transit, storing it in an encrypted format, and securing your encryption keys in Apple data centers. Both Apple and third-party data centers may be used to store and process your data. When processing data stored in a third-party data center, encryption keys are accessed only by Apple software running on secure servers, and only while conducting the necessary processing.

End-to-end encryption

For additional privacy and security, many Apple services use end-to-end encryption, which encrypts your information using keys derived from your devices and your device passcode, which only you know. This means that only you can decrypt and access your information, and only on trusted devices where you’re signed in with your Apple ID. No one else, not even Apple, can access your end-to-end encrypted data. End-to-end encryption requires two-factor authentication for your Apple ID and a passcode set on your devices. Some features using end-to-end encryption may require up-to-date software.

Data types and encryption

Here's more detail on how iCloud protects your data and which data types use end-to-end encryption.

Data	Encryption	Notes
Backup	In transit & on server	A minimum of 128-bit AES encryption
Calendars	In transit & on server	
Contacts	In transit & on server	
iCloud Drive	In transit & on server	
Notes	In transit & on server	
Photos	In transit & on server	
Reminders	In transit &	

	on server	
Safari Bookmarks	In transit & on server	
Siri Shortcuts	In transit & on server	
Voice Memos	In transit & on server	
Wallet passes	In transit & on server	
iCloud.com	In transit	All sessions at iCloud.com are encrypted with TLS 1.2. Any data accessed via iCloud.com is encrypted on server as indicated in this table.
Mail	In transit	All traffic between your devices and iCloud Mail is encrypted with TLS 1.2. Consistent with standard industry practice, iCloud does not encrypt data stored on IMAP mail servers. All Apple email clients support optional S/MIME encryption.
Apple Card transactions	End-to-end	
Health data	End-to-end	Additional info below
Home data	End-to-end	
Keychain	End-to-end	Includes all of your saved accounts and passwords
Maps Favorites, Collections and search history	End-to-end	
Memoji	End-to-end	
Messages in iCloud	End-to-end	Additional info below
Payment information	End-to-end	
QuickType Keyboard learned vocabulary	End-to-end	
Safari History, Tab Groups, and iCloud Tabs	End-to-end	
Screen Time	End-to-end	
Siri	End-to-end	Includes Siri settings and personalization, and if you have set up Hey Siri, a small sample of your requests

Wi-Fi passwords	End-to-end	
W1 and H1 Bluetooth keys	End-to-end	

Messages in iCloud

For Messages in iCloud, if you have iCloud Backup turned on, your backup includes a copy of the key protecting your messages. This ensures you can recover your messages if you lose access to your Keychain and your trusted devices. When you turn off iCloud Backup, a new key is generated on your device to protect future messages and isn't stored by Apple.

Health data

If you use your Mac to back up your device, Health data is stored only if the backup is encrypted. Learn more about managing your Health data.

Recovering your iCloud data

If you forget your Apple ID password or device passcode, there are several methods for recovering the data that you store in iCloud.

iCloud Data Recovery Service

If you forget your password or device passcode, iCloud Data Recovery Service can help you decrypt your data so you can regain access to your photos, notes, documents, device backups, and more. Data types that are protected by end-to-end encryption—such as your Keychain, Messages, Screen Time, and Health data—are not accessible via iCloud Data Recovery Service. Your device passcodes, which only you know, are required to decrypt and access them. Only you can access this information, and only on devices where you're signed in to iCloud.

Account recovery contact

An account recovery contact is a person who you know and trust and who can verify your identity and help you regain access to your iCloud data—including your end-to-end encrypted data—if you ever get locked out. Your recovery contact doesn’t have access to your account, only the ability to give you a code if you need one. Learn how to set up an account recovery contact.

Account recovery key

A recovery key is a randomly generated 28-character code that you can use to help reset your password or regain access to your Apple ID. Using a recovery key means that you’re responsible for maintaining access to your trusted devices and your recovery key. If you lose both of these items, you could be locked out of your account permanently even if you have a recovery contact. Learn how to generate a recovery key.

Privacy

Apple believes that privacy is a human right. Our Privacy Policy covers how we collect, use, disclose, transfer, and store your information. And in addition to adhering to the Apple Privacy Policy, Apple designs all iCloud features with your privacy in mind.

Learn more

To learn more about advanced security features in Apple products, visit Apple platform security.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Contact the vendor for additional information.

Published Date: September 27, 2022